REMARKS

Claims 3, 6-10, 15-17, and 19-30 are pending in the application and stand rejected.

Rejection under 35 U.S.C §102

Claims 26 and 29 stand rejected under 35 U.S.C. 102(b) as being anticipated by WIPO Patent Publication No. 98/44402 to Bramhill et al. The Examiner explains that:

> Bramhill discloses a server that securely sends data to an authenticated client. This inherently requires the server to have a memory from which an image of the program having this functionality can be executed. The authentication of the token may involve the use of a token sent to the client to verify that the client has permission and has not been tampered, ensuring that the client restricts use of the data (such as image data, which is displayed at a client) before it is sent.

Applicants respectfully submit that the above does not set forth a proper §102 rejection because it does not show that each and every claimed limitation is disclosed by Bramhill. Claim 1 recites, *inter alia*, means to authenticate a trusted component of a client platform, the trusted component having a display controller such that display of the data from the server is controlled from within the client trusted component. There is nothing in Bramhill that can be understood as disclosing a trusted component of a client platform. There is also nothing in Bramhill that discloses or alludes to a display controller such that display of data is controlled from within the client trusted component. Applicants have previously explained that at most, Bramhill discloses that the client machine runs a Java-enabled browser that has the right mouse buttons disabled for a region displaying a particular image (i.e. the well known "save as", etc.). A Java-enabled browser is software and certainly does not read upon a trusted component (which is clearly hardware) having a display controller such that display of the data from the server is controlled from within the client trusted component.

Furthermore, Bramhill discloses that the authentication of the client may be done through a so-called dogtag program which is provided to the user through the mail to thereby ensure that the correct user receives is and thus provide "reasonable certainty" that the client machine

running the dogtag program correspond to the correct user. Nevertheless, such a dogtag program also fails to anticipate the presently disclosed trusted component with display controller because (1) a program is not a component with a display controller, and (2) regardless, there is no disclosure whatsoever that the dogtag program can control the display of information on the client machine.

Claim 26 further recites that the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code. The Examiner notes that the server of Bramhill does not provide data to a client unless the client is authenticated. However, there is nothing in Bramhill that teaches that authentication of a client determines that the client platform is adapted to ensure restricted use of the data. At page 11 Bramhill teaches that a client may be authenticated if it has made a payment, or if it known to the server in respect of some other service being provided and "the client's *credentials* may be authenticated by means of procedures already in use for the service." Neither of these types of authentication have any bearing upon determining that the client platform is adapted to ensure restricted use of the data - at best, they determine that the client platform has paid for use of the data. Similarly, the dogtag program exists solely "to provide a machine identification code (MID) which provides a substantially unique identification of the client." The dogtag program has no control whatsoever upon the display of data. Again, the only control over the display of the data is accomplished through the Java-enabled browser, and this browser does in no way anticipate a client trusted component having a display controller such that display of the data from the server is controlled from within the trusted component. Furthermore, Applicants note that claim 26 recites means to *authenticate* such a trusted component, and there is nothing in Bramhill that discusses means on the server for authenticating the Java-enabled browser on a client.

Claim 29 similarly recites a server determining that the client platform both has permission to receive image data, and has a client trusted component physically and logically protected from unauthorized modification adapted to use the image data only for the restricted use and to control display of the image data from within the client trusted component. As explained above, there is no such client trusted component to be found in Bramhill, but rather

only a Java-enabled browser that cannot be understood as being a "component physically and logically protected from unauthorised modification."

Applicants further disagree with the Examiner's assertion that "The authentication of the token may involve the use of a token sent to the client to verify that the client has permission and has not been tampered" because (1) there is no token mentioned in Bramhill, (2) there is nothing akin to a token mentioned in the claims, and (3) as explained above, there is no discussion whatsoever in Bramhill of checking whether a client has been *tampered* with - only whether the client has paid a sum of money in order to be allowed to view a picture.

In view of the above, Applicants respectfully submit that claims 26 and 29 are in fact novel and nonobvious over Bramhill and request the Examiner to kindly reconsider and withdraw this rejection.

Rejections under 35 U.S.C §103

Claims 8 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,879 to Davis in view of U.S. Patent No. 5,517,569 to Clark. In particular, the Examiner finds that, with regard to claim 25, Davis discloses all of the claimed limitations with the exception of a mechanism for verifying the integrity of the platform upon user request, that Clark discloses a hardware test in a protected platform in which a user may initiate the verifying the platform's integrity, and concludes that it would have been obvious to a skilled person to modify the invention of Davis by implementing it with a user-initiated integrity check as disclosed by Clark so that a user may have confidence in the platform that he or she is using. Applicants respectfully disagree.

The Examiner asserts that Davis discloses a trusted component logically protected from unauthorized modification at col. 3 ll. 27-43 and offers the explanation "protected key loading." Applicants have reviewed this passage, which is reproduced below, and simply cannot understand what the Examiner means by "protected key loading":

> In exchange for payment, or some other mutually agreed upon arrangement, the provider transfers a cryptographic key either to the SVCP directly through a

> connecting cable (e.g. telephone lines, cable, etc.) or to the user who subsequently loads the cryptographic key into the SVCP. The cryptographic key is needed for decoding the video to be viewed. The cryptographic key may be encrypted with the public key of the SVCP to ensure its security. Along with the needed cryptographic key, other authorization information may also be transferred. Such information may include, but is not limited to, the number of times a video may be watched or an expiration time upon which the video may no longer be watched. Thus, the encrypted video itself is useless without the cryptographic key, allowing the encrypted video to be provided by the provider or by other general distribution sources such as the internet.

This passage teaches that a cryptographic key must be loaded into the secure video content processor (the SVCP, which the Examiner asserts to read upon the presently claimed trusted component), and that this may be done directly through a cable or entered by a user through a keyboard. Applicants simply cannot understand why the Examiner interprets this as teaching that the SVCP is logically protected from unauthorized modification. The cryptographic key that is the subject of this passage is required for the SVCP to decrypt a particular video stream to be able to play it; the need for such a key certainly offers no logical protection against unauthorized modification, rather it offers protection of the video stream against unauthorized display. Applicants submit that the Examiner has misinterpreted the teachings of this passage and respectfully invite him to review this passage and reconsider his interpretation or provide a clearer explanation of this interpretation.

Applicants further disagree with the Examiner's rationale for combining the Davis and Clark references. The Examiner asserts that the skilled person would recognize that it is important for a user to have confidence in the platform that he or she is using, but offers not one iota of support for this broad assertion. "Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some *rational underpinning* to support the legal conclusion of obviousness." *In re Leonard Kahn*, 04-1616, *p. 15 (Fed. Cir., March 22, 2006) [emphasis added]. The Davis reference is concerned with preventing unauthorized reproduction of a video distributed via the Internet, and solves the problem by providing a secure video content processor that is incorporated in the end-user's

client platform (e.g. PC, set-top box, video game console) and forces the user to pay the video content provider before enabling the display of the video on the user's platform. Applicants submit that the skilled person looking to implement this system would not be concerned with whether the user has confidence in his platform - after all, this platform is typically in the user's own bedroom or living room where there is no fear of unauthorized access to the platform. The entire raison d'être of Davis is to protect the video distributor, not the end user, and contemplating the addition of a platform verification option does nothing to further this purpose (protecting the distributor), and Applicants therefore disagree that there is any motivation for the skilled person to modify Davis' invention as asserted by the Examiner.

Furthermore, even if moved to implement the hardware testing feature of Clark into the system of Davis, there is simply no reason in the references or in common sense to implement it in the SVCP. "The SVCP is usually included within a video subsystem 116 implemented inside a PC 100, usually on a PCI bus compatible card much like a traditional graphics controller card." (col. 4 l. 21) Clark's hardware test operation 420 is one of quite a few software subroutines (menu options) within a remote transaction application program. Why would the skilled person lift one such subroutine out of this program and implement it within an ASIC on a graphics controller card? There is nothing in the references nor in the Examiner's discussion that would explain why the skilled person would take the much more complex and expensive route of implementing Clark's application program in the hardware of Davis, and Applicants submit that the skilled person would at most provide the same application program to run on the user platform of Davis.

Finally, Applicants note that the Examiner has also failed to make a showing of the requisite reasonable expectation of success for a proper §103 rejection as set forth in MPEP §2142: "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure."

Finally, Applicants disagree that "by authenticating the received data, Davis' client in effect verifies the trusted status of another platform, the server" because Davis' client does not authenticate received data, it decrypts it. Furthermore, the Examiner offers no explanation how

authenticating data received from a server verifies the trusted status of that server - and Applicants submit that in fact it cannot; authenticating received data simply verifies the source of the data, not a trusted status of that source.

In view of all of the above, Applicants respectfully submit that claims 25 and 8 are in fact non-obvious and patentable over Davis and Clark and request the Examiner to kindly reconsider and pass these claims to issue.

Claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 further stand rejected under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claim 26 and further in view of Davis and further in view of Clark. Applicants respectfully disagree and submit that the previous discussion of Bramhill and Davis, wherein Applicants have explained that these references each omits at least one claimed element contrary to the Examiner's assertion, are equally probative of the non-obviousness and patentability of these claims over the combination of Bramhill, Davis and Clark. Specifically, Davis does not in fact disclose a trusted component with display controller as claimed, and even if applying Davis' tamper-proofing at the client to Bramhill, the skilled person would still not obtain a client trusted component physically and logically protected from unauthorized modification to provide verification of the integrity of the platform to a user upon user request and further having a display controller such that the display is controlled from within the client trusted component.

Furthermore, the Examiner's proffered motivation to combine the two references does not make complete sense - why would the skilled person add the significant expense and complexity of tamper-proofing the client hardware as per Davis when Bramhill already "makes it more difficult to capture the unencrypted digital representation" by disabling select software functions in the client platform? Although Davis and Bramhill are concerned with the same problem (preventing unauthorized distribution of digital content), they provide completely different solutions - Bramhill downloads an applet together with the content that controls the user's platform to the extend the content is displayed, whereas Davis provides specific hardware on the user's platform. These are completely opposite approaches to the same problem, and combining them is no easy feat nor advantageous from an engineering point of view - and the

Examiner has once again not made a showing of why the skilled person would have a reasonable expectation of success when attempting to combine these two radically different solutions. Applicants submit that the motivation asserted by the Examiner to combine these two references, "to make it more difficult to capture the unencrypted digital representation," simply does not exist outside of the Examiner's hindsight because making it more difficult to capture the unencrypted digital representation is the very purpose of Bramhill and the skilled person has no reason to look to another reference for another solution to the same exact problem.

Applicants also once again note that there is a similar lack of motivation to add the Clark reference to the mix, as fully detailed above. Applicants thus respectfully submit that claims 3, 6, 9, 15-17, 19-22, 25, 28 and 29 are in fact non-obvious and patentable over the art on record and request the Examiner to kindly withdraw this rejection as well.

Claims 10, 23 and 24 further stand rejected under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claims 26 and 29 and further in view of Davis and Clark and further in view of U.S. Pat. No. 5,990,927 to Hendricks. Claims 7 and 27 further stand rejected under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claims 26 and 29 and further in view of Davis and Clark and further in view of U.S. Pat. No. 6,219,788 to Flavin. Applicants once again invoke the above discussion of Bramhill, Davis, and Clark and submit that this discussion is equally probative of the non-obviousness and patentability of these claims over the combination of Bramhill, Davis, Clark and Hendricks or Flavin, because claims 7, 10, 23, 24 and 27 depend from claims that have been shown above to be patentable.

Claim 30 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Bramhill as applied to claim 26 and further in view of Davis and U.S. Pat. No. 5,355,414 to Hale et al. Again, Applicants submit that the combination of Bramhill and Davis is not in fact obvious to the skilled person. Furthermore, Hale does not in fact teach locking a user interface, contrary to the Examiner's assertion:

> In one embodiment, the host computer is in communication with a display, and the peripheral device controller is further responsive to the predetermined period during which the peripheral input device remains inactive to send signals to the host to deactivate the display so that information visible on the display is not viewable. In this embodiment, the peripheral input device is further responsive to the predesignated signals from the peripheral input device to restore operation of the display. [col. 3, ll. 27-33, cited by the Examiner]

The above teaches deactivating a display - how can this possibly be understood as locking a user interface? A user interface consists of a display and at least an input device (keyboard, mouse, etc.). Locking such an interface clearly means preventing the user from interfacing with the platform including preventing input by the user. Where is any of this even alluded to in Hale?

Furthermore, why would the skilled person implementing Bramhill's or Davis' systems care to prevent the display of insecure information? Where could such "insecure information" possibly come from in Bramhill or Davis? What possible benefit could be added to either Bramhill or Davis, which are specifically concerned with very strictly controlling the display of certain data, by endowing it with the ability to lock the interface to the user's platform? For that matter, what user would care to download data from a server using either Bramhill or Davis' invention if the user interface on his platform could be locked by the server? Adding this feature to either Bramhill or Davis simply makes no sense, and Applicants respectfully submit that claim 30 is non-obvious and patentable over the art on record and request the Examiner to kindly also withdraw this rejection.

Applicants finally wish to address the Examiner's contention of page 10 that "Though the client disclosed by Bramhill is not as well-protected as that of the instant application, it nonetheless constitutes a trusted component insofar as the term is defined in the instant application's specification." As was shown above, this is not true because there is nothing in Bramhill that even briefly mentions any hardware on a client platform. The teachings of Bramhill have absolutely no impact upon the client platform beyond the disabling of a few

Internet browser functions by a downloaded applet. The Examiner's assertion that this constitutes a trusted component insofar as the term is defined in the instant application's specification is simply untenable, and the Examiner may wish to review the specification at, *inter alia*, p. 5 ll. 6-14 and p. 9 l. 30 - p. 10 l. 10 for examples of the definition of the term "trusted component."

* * *

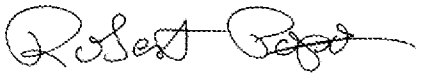
In view of all of the above, Applicants submit that the application is in condition for allowance and respectfully urge the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

September 14, 2007
(Date of Transmission)

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@la.ladas.com